UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/706,829	11/12/2003	Kyung-Duck Seo	8836-205 (IB12086-US)	6940

22150 7590 11/28/2007
F. CHAU & ASSOCIATES, LLC
130 WOODBURY ROAD
WOODBURY, NY 11797

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
11/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/706,829	**Applicant(s)** SEO, KYUNG-DUCK	
	Examiner Carl Colin	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *see att*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In communications filed on 9/10/2007, applicant amends claim 9, the following claims 1-14 are presented for examination.

1.1 In response to communications filed on 9/10/2007, Applicant has amended the specification to overcome the objection from the last Office Action, the objection to the specification and claim 9 has been withdrawn with respect to the amendments.

1.2 Applicant's remarks, pages 7-10, filed on 9/10/2007, with respect to the rejection of claims 1-14 have been fully considered but they are not persuasive. Applicant argues that Sprunk does not explicitly disclose that the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion process. However, as explained in the last office action Gligor et al discloses this limitation. Applicant argues that Sprunk discloses a single processor and does not teach two encryption devices. Examiner respectfully disagrees as the claim does not explicitly recite two encryption devices. In addition, the functions described for converting the input data block and the key may be software such as lookup tables or hardware such as digital circuits that meets the recitation of device (see column 4, lines 4-7). Contrarily to applicant's arguments about Gligor, Gligor et al discloses first and second devices performing cryptographic conversion in parallel (paragraphs 4-5) and Sprunk suggests applying the functions into any of the input port and output port or combination thereof (see column 4, lines 4-15). Therefore, the combination of Sprunk and Gligor et al discloses first and second N-round DES devices performing a substantially simultaneous cryptographic conversion process. Upon further consideration, Applicant has not overcome the rejection in view of Sprunk and Gligor et al and the rejection is set forth below.

Information Disclosure Statement

2. The information disclosure statement filed on 11/5/2007 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in the English language. It has been placed in the application file, but the information referred to therein has not been considered.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,473,693 to **Sprunk** in view of US Patent Publication US 2002/0048364 to **Gligor et al**.

As per claim 1, **Sprunk** substantially discloses an encryption apparatus comprising: a first N-round DES device for cryptographically converting a digital input data block (X) into a first digital output data block nonlinearly, based on an input of a set of encryption keys (K) (see column 3, lines 30-41 and fig.1); a first input means for receiving and inverting the digital input data block (see column 3, lines 26-30 and column 5, lines 43-53); a second input means for receiving and inverting the set of encryption keys (see column 3, lines 26-30 and column 5, lines 43-53); and a second N-round DES device for cryptographically converting the inverted digital input data block into a second digital output data block nonlinearly, based on an input of the set of inverted encryption keys (see column 5, line 49 through column 6, line 5), **Sprunk** suggests applying the functions (conversion) into any of the input port and output port or combination thereof (see column 4, lines 4-15). **Sprunk** does not explicitly disclose wherein the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion process. **Gligor et al** in an analogous art teaches parallel block encryption suitable for real-time applications and further discloses that parallel processing offers significant advantages of executing block enciphering and deciphering operations; for instance, incremental and out-of-order processing on a per block basis as opposed to that on a per-segment basis has the advantage of lower processing overhead (see page 1, paragraphs 4-5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of **Sprunk** to provide parallel processing as suggested by **Gligor et al** to benefit from lower processing overhead and separate encryptions can be applied in a single pass (paragraph 12).

As per claim 7, **Sprunk** substantially discloses method of cryptographically converting digital input data comprising the steps of: cryptographically converting a digital input data block (X) into a first digital output data block nonlinearly, based on an input of a set of encryption keys (K) (see column 3, lines 30-41 and fig.1); inverting the digital input data block and the set of encryption keys (see column 3, lines 26-30 and column 5, lines 43-53); and cryptographically converting the inverted digital input data block into a second digital output data block nonlinearly, based on an input of the inverted encryption keys (see column 5, line 49 through column 6, line 5), **Sprunk** suggests applying the functions (conversion) into any of the input port and output port or combination thereof (see column 4, lines 4-15). **Sprunk** does not explicitly disclose wherein the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion process. **Gligor et al** in an analogous art teaches parallel block encryption suitable for real-time applications and further discloses that parallel processing offers significant advantages of executing block enciphering and deciphering operations; for instance, incremental and out-of-order processing on a per block basis as opposed to that on a per-segment basis has the advantage of lower processing overhead (see page 1, paragraphs 4-5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of **Sprunk** to provide parallel processing as suggested by **Gligor et al** to benefit from lower processing overhead and separate encryptions can be applied in a single pass (paragraph 12).

As per claim 9, **Sprunk** substantially discloses an encryption apparatus having a substantially uniform current pattern during cryptographic processes comprising: a first N-round DES device producing a first current pattern during cryptographic process on a digital input data block (X), based on an input of a set of encryption keys (K) (see column 3, lines 30-41 and fig.1); and a second N-round DES device producing a second current pattern during cryptographic process on an inverse of the digital input data block, based on an input of the set encryption keys in inverted form (see column 5, line 49 through column 6, line 5), **Sprunk** suggests applying the functions (conversion) into any of the input port and output port or combination thereof (see column 4, lines 4-15). **Sprunk** does not explicitly disclose wherein the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion process. **Gligor et al** in an analogous art teaches parallel block encryption suitable for real-time applications and further discloses that parallel processing offers significant advantages of executing block enciphering and deciphering operations; for instance, incremental and out-of-order processing on a per block basis as opposed to that on a per-segment basis has the advantage of lower processing overhead (see page 1, paragraphs 4-5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of **Sprunk** to provide parallel processing as suggested by **Gligor et al** to benefit from lower processing overhead and separate encryptions can be applied in a single pass (paragraph 12).

As per claims 2 and 10, **Sprunk** discloses wherein the first and second N-round DES devices perform a cryptographic conversion process according to a DES algorithm, respectively (see figures 1 and 2 and abstract).

As per claims 3 and 11, **Sprunk** discloses means for storing the first and second digital output data blocks from the first and second N-round DES devices (see column 5, lines 9-10), either one of the first and second digital output data blocks being used as an encryption data block (see column 4, lines 4-15).

As per claims 4 and 12, **Sprunk** discloses the limitation of further comprising a third input means for transferring the digital input data block to the first N-round DES device (see column 3, lines 30-41 and fig.1).

As per claims 5 and 13, **Sprunk** discloses an encryption key block for receiving a key and generating the set of encryption keys based on a permutation of the key (see column 5, lines 19-23).

As per claims 6 and 14, **Sprunk** discloses a fourth input means for transferring the set of encryption keys to the first N-round DES device (see column 3, lines 30-41 and fig.1).

As per claim 8, **Sprunk** discloses wherein either one of the first and second digital output data blocks being used as an encryption data block (see column 4, lines 4-15).

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the prior art discloses conversion of input to output with inverse transformation. (See PTO-form 892).

4.1 **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

4.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/

Carl Colin

Patent Examiner, A.U. 2136
November 26, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/26/07